Monterey Technology Group, Inc.

SEMINARS

Security Log Secrets

Course Description

The Windows security log is extremely important to monitoring all aspects of Windows security but it's safe to say the Windows security log is the most poorly documented area of Windows 2000 and Windows Server 2003. For most events, Microsoft documentation simply restates the static text of the event's description. Where there is information, it's riddled with inaccuracies. But more importantly, there is almost no guidance and very little background information for individual events much less events in context with other events. There are no "suggested courses of action", "what this event means if it has ... or is accompanied by events ...". Furthermore, the security log event IDs and codes change from one version to the next in Windows which makes security log knowledge even more arcane and complicates the design of programs that monitor the security log.

Overview

- Introduction To Windows Security Logging
- Monitoring Logon & Authentication Events
- Monitoring User Activity
- Auditing Admins & Account Maintenance
- Auditing System Activity
- Automating Log Monitoring & Archiving

(See next page for detailed course outline.)

Monterey Technology Group, Inc.

Security Log Secrets

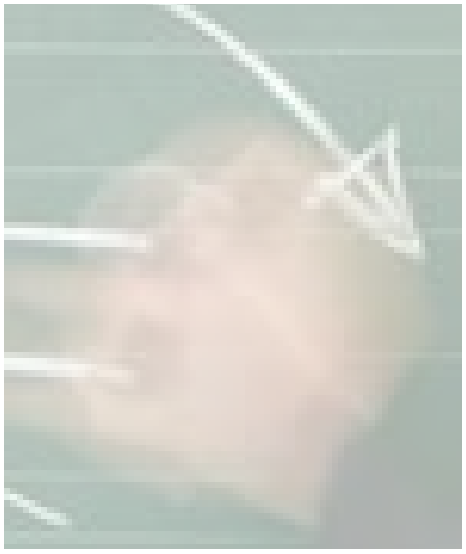
What You Will Learn

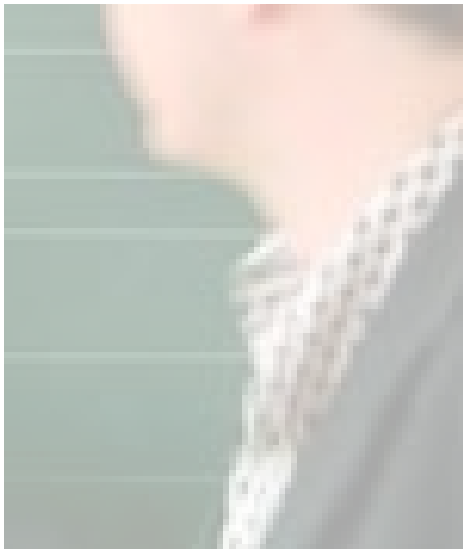
In this intensive, 2-day course you will explore all 9 audit categories of Windows Server 2003 and learn about the subtle differences between 2003, 2000 and XP security events. You will learn how to monitor logon activity across your domain. You will find out how to determine when a user logged on, which workstation they were at and which servers they tried to access. You'll learn how to distinguish between local and domain account logon attempts. You will see how to track which programs a user executes on his workstation and which files he accesses on the server, what type of access he gained to the files and whether he actually changed any data using operation based auditing. You will learn why Windows 2000 can't tell you whether a user who opened a file for write access actually updated the file or just closed it without making changes. And you'll discover how Windows Server 2003 addresses this limitation.

Individuals with administrator or other high levels of authority need monitoring just as much if not more than end users. You will learn how to track administrative and help desk activity including user account maintenance, password resets, group membership changes and more. You will also discover how to audit changes to Active Directory objects down to the property level. While it may be difficult, it's not impossible to tamper with the security log. You'll find out how to detect potential tampering and measures you can implement to prevent log tampering. You'll learn what each event ID means and how to interpret the obscure codes and other data in event descriptions. You will learn how to used the security log to facilitate compliance with the monitoring requirements of Sarbanes-Oxley, GLBA, HIPAA and SEC rules.

What You Will Take Back

One of the most challenging factors in effectively monitoring Windows is the fact that each system has its own security log containing its discrete portion of your network's overal security activity. Randy will show you how to automate the process of merging, monitoring and analyzing the many security logs in your network using a variety of example scripts, techniques and free tools from Microsoft and other. Randy will also discuss important evaluation criteria and architectural factors to consider when selecting an event log monitoring solution.





Monterey Technology Group, Inc.

866-749-2048 voice • 864-574-0219 fax

www.montereytechgroup.com • www.ultimatewindowssecurity.com

Monterey Technology Group, Inc.

Security Log Secrets

Course Agenda

1. Introduction to Windows Security Logging
- System audit policy
- Event viewer
- Maximum log size and overwrite options
- Frequently held misconceptions
- Using group policy to configure audit policy and event log settings

2. Introduction to LogParser
- Architecture
- SQL engine
- Output formats
- Using LogParser with the Windows security log

3. Understanding Authentication and Logon
- Authentication vs. Logon
- Local Accounts vs. Domain Accounts
- Authentication Protocols
- NTLM
- Kerberos

4. Logon/Logoff Events
- Audit logon events
- Logon types
- Successful logon events
- Logon failure events
- Logon IDs
- Tracking logoff events
- Changes in Windows Server 2003
- Sample LogParser scripts

5. Account Logon Events
- Relationship to Logon/Logoff events
- NTLM events
- Kerberos events
- Centrally tracking domain authentication
- Monitoring local account authentication attempts
- Changes in Windows Server 2003
- Sample LogParser scripts

6. Object Access Events
- Audit object access events
- Object level audit policy
- File and folder auditing
- Auditing file modifications
- Detecting unauthorized access attempts
- Auditing services, registry keys and other objects
- Operation based auditing in Windows Server 2003

7. Detailed Tracking Events
- Audit process tracking
- Tracking executables
- Linking process events to logon/logoff events
- Process ID and Creator Process ID

8. Account Management Events
- Audit account management
- Tracking help desk and admin activity
- Monitoring changes to user accounts
- Tracking new computer accounts
- Auditing group membership changes
- Detecting changes to administrator authority
- Sample LogParser scripts
- Changes in Windows Server 2003

9. Directory Service Access Events
- Audit directory service access
- Comparison to Account Management events
- Active Directory Schema
- Tracking changes to organizational units and domains
- Auditing maintenance of group policy objects
- Changes in Windows Server 2003

10. Auditing System Activity
- Audit privilege use events
- Audit system events
- Audit policy change events
- IPSec, EFS and certificate events
- Selective user auditing

11. Recommended Monitoring and Reporting
- Key security log events and their uses
- Authentication and logon events
- Account management events
- File and object access events
- Active Directory events
- System activity events
- Policy change events

12. Relating the Security Log to Compliance
- SOX
- GLBA
- HIPAA
- Basil II
- Change control
- Access control
- Intrusion detection
- Privacy
- Integrity
- Confidentiality, integrity and availability

13. Automating Log Management
- Selecting the right event log management solution
- Collection
- Alerting
- Reporting
- Archival
- Log management evaluation criteria
- Description field handling
- Agent-based vs. agentless
- Network and database security
- Separation of duty
- Getting the most from your event monitoring solution

FAQ

Why do I need this course? Isn't the security documented by Microsoft and other sites?
For most events, Microsoft's documentation simply restates the static text of the event's description. While some information does exist, it's riddled with inaccuracies. Most important, there is insufficient guidance and very little background information for individual events, nor are events described in context with other events. Further, there are no suggested courses of action.

Other sites are valuable but only provide basic information about individual event IDs. To perform any of the substantive analysis, auditing or monitoring you need to understand the relationship between related event IDs, know the patterns to look for and how to relate event IDs to their respective control areas in Windows security configuration. The Security Log Secrets course will enable you to overcome the limitation of poor documentation by providing you the knowledge to manage and respond to issues relative to your Windows installations.

Will this course help me with compliance efforts?
Yes, you will learn how to identify and retrieve key types of compliance monitoring data such as change control, changes in privileged access and authority, unauthorized attempts to access confidential information or modify financial data.

We just purchased a security log management solution. Aren't its pre-built alert rules and reports good enough?
Usually not. There are many security log management solutions on the market that offer good infrastructure technology for managing the security log. Typically, software developers are good at developing software but are not experts on the cryptic Windows security log. Consequently, most pre-built alert criteria and reports are proof-of-concept examples or at best they help with minor issues. They do not perform the necessary task of compiling data for strategic management of the enterprise.

How did Monterey Technology Group develop the Security Log Secrets course?
Randy Franklin Smith, CEO of Monterey Technology Group, began researching the Windows security log in 1998 for a client project. Due to the lack of accurate documentation, Randy reverse-engineered every event ID in the security log along with the codes and other detailed fields within each event. Along the way Randy developed an understanding of events in relation to each other and been able to link user and administrator level actions with patterns of events. Since then he has provided design consultation to developers of event log monitoring products and written over a dozen articles on the subject, several of which now reside on Microsoft's Technet website. Because of constant interest from readers, Mr. Smith decided to create Security Log Secrets seminar as an in-person venue for sharing the results of years of research and helping attendees implement effective monitoring, compliance auditing, forensic analysis and intrusion detection.

Monterey Technology Group, Inc.

866-749-2048 voice • 864-574-0219 fax
www.montereytechgroup.com • www.ultimatewindowssecurity.com

Randy Franklin Smith, CEO
Monterey Technology Group Inc

Randy is a Systems Security Certified Professional (SSCP) who specializes in Windows and Active Directory security. He performs security reviews for clients ranging from small, privately held firms to Fortune 500 companies, national, and international organizations.

Additional Certifications

- Microsoft Security MVP
- Certified Information Systems Auditor (CISA)

Industry Memberships

- Information Systems Security Association (ISSA)
- Information Systems Audit and Control Association (ISACA)
- Technology Association of Georgia (TAG)
- Center for Internet Security (CIS)

Training Experience

Randy is the designer and exclusive instructor for the Ultimate Windows Security seminars:

- Security Log Secrets
- Total Wi-Fi Security
- Complete Windows Security

Prior to designing his extensive security seminars, Randy accrued many years of experience training IT auditors on Windows security as the developer and primary instructor for MIS Training Institute's Windows and audit curriculum.

Each year through MIS, Randy still trains dozens of internal auditors from organizations around the world, including:

- The "big four" public accounting firms
- Bank examiners with the FDIC, OCC, OTS
- NASA and the OAS

Information Security Author

Randy has written over 300 articles on Windows security issues, which appear in publications like Information Security Magazine and Windows IT Pro where he is a contributing editor and author of the popular Windows security log series. In 2003 Randy received the Apex Award of Excellence in the category of How-to Writing for his security feature "8 Tips for Avoiding the Next Big Worm." He is also technical editor of Security Administrator where he writes the popular Access Denied Q&A column.

Monterey Technology Group, Inc.

866-749-2048 voice • 864-574-0219 fax
www.montereytechgroup.com • www.ultimatewindowssecurity.com